McKenzie, R. N., McNulty, G. F. and Taylor, W. F., *Algebras, lattices, varieties,* Volume I (Wadsworth & Brooks/Cole, Monterey, California 1987) xii+361 pp. 0 534 07651 3, $44.95.

This book is the first volume in a planned four volume survey of the theory of general algebras. A general algebra is a non-empty set equipped with a system of finitary operations. This is a very general concept and it has as special cases the theory of many familiar algebraic structures: groups, rings, fields, vector spaces, modules, near-rings, non-associative algebras etc. What is perhaps a bit surprising is how much can be done in this very general context. There have been several textbooks on this subject over the years, notably by G. Birkhoff, P. M. Cohn, G. Gratzer, A. G. Kurosh, B. Jonsson and A. I. Mal'tsev among others. This series of four volumes aims to provide a thorough survey of the present state of the theory, including many powerful new areas of research that have only recently been developed.

Volume I is the introductory work, providing the basic results and tools. The first chapter sets the scene and lays the foundations. The second chapter is concerned with lattices. This has been one of the key tools in general algebra right from the beginning and is a subject often neglected in the education of algebraists. Here there is a very good introduction to the subject. There follows a chapter on unary and binary operations, the ones which occur most commonly, and which turn out to have a special importance in the general theory. The next chapter, entitled Fundamental Algebraic Results, covers a wide variety of fundamental ideas and techniques, including some only recently developed such as commutator theory. Up to this point, we have the introductory text on general algebra. The last chapter is devoted to the study of unique factorization in algebras. The theme of this study is the question of how unique is a factorization of an algebra into a direct product of indecomposable algebras. Some very general results are presented which have as corollaries many known results about uniqueness of decompositions.

The most interesting aspect of this book is to see how so many familiar results are simply special cases of a much more general theorem. The latest example is the commutator theory developed for general algebras in chapter four. For anyone wishing to have a bird's eye view of algebra as a whole, and to get a feel for the exciting developments now taking place in general algebra, this book is a good starting point. It is well presented with a lot of exercises for the keen reader and the contents are well-organized. At times, it can be a bit dry and remote, but that is probably inevitable in this subject. It will be a very useful reference work, and I look forward to the remaining volumes in the series. The quality of production is very good and the price very reasonable for a book at this level.

J. D. P. MELDRUM

Patterson, S. J., *An introduction to the theory of the Riemann zeta-function* (Cambridge studies in advanced mathematics 14, Cambridge University Press 1988), 156 pp. 0 521 33535 3, £20.

During the last few years a number of books on the Riemann zeta-function have appeared, and it might be thought that there was little need for yet another text. However, Patterson's book differs from its predecessors in several interesting ways, and primarily in that in it a central role is played by the Poisson summation formula. The author stresses in his preface that the book *is* intended as an introduction to the theory of the zeta-function, suitable for a reader with a good undergraduate background in analysis and elementary number theory. Here analysis is the operative word, since the arguments presented demand considerable analytical expertise, and even, perhaps, maturity on the part of the reader.

The book contains six chapters, beginning with an illuminating historical introduction. After this the Poisson summation formula and the functional equation are derived. Next come the explicit formulae of prime number theory, a study of the zeros and the Prime Number Theorem,

https://doi.org/10.1017/S0013091500028753 Published online by Cambridge University Press

followed by a very detailed consideration of the Riemann and Lindelöf hypotheses, and finally a chapter on the approximate functional equation. There are seven appendices covering such general topics as Fourier theory, the gamma function and the Phragmén–Lindelöf theorem.

The author's knowledge both of the history of his subject and modern developments is impressive and a reader who has studied the book in detail will find that he has acquired a deeper appreciation of the theory. Some parts of the chapter on the Riemann hypothesis have been asterisked to indicate that they require a background of algebraic geometry. These are undoubtedly the most difficult parts of the book, while at the same time being the most valuable for any mathematician intending to carry out research in the area.

At the ends of each chapter and of several of the appendices there are numerous exercises. There are a number of misprints and minor errors, which should be easily corrected.

R. A. RANKIN

KOBLITZ, N., *A course in number theory and cryptography* (Graduate Texts in Mathematics 114, Springer-Verlag, Berlin–Heidelberg–New York 1987) viii + 208 pp. 3 540 96576 9, DM 74.

As a human activity, cryptography has a long and fascinating history, going back probably almost as far as writing itself. As a branch of mathematics, however, it is a newcomer. And while mathematical and statistical ideas have been used for some time for breaking secret codes, the use of number theoretic methods for the construction of codes is a very recent development. It has enabled teachers and grant applicants to sell number theory as an area of mathematics with applications, and has brought an unprecedented amount of computing power and expertise into the subject. (The fact that much of this power is directed towards finding good factoring algorithms is somewhat ironic, for if really good factoring algorithms were found, most number-theory-based crypto-systems would be fatally weakened, and practical applications of number theory to cryptography would largely disappear!) This brings us to the main difficulty of regarding cryptography as a respectable branch of mathematics: its dearth of theorems on the strength of cryptosystems. While number theory can be used to construct cyphers, we have no proof of their security, and so no real idea at present whether number theory is to have a lasting place in cryptography.

The text under review gives us, in the author's typically clear style, firstly the number theory we need, followed by chapters on simple cryptosystems, public key ciphers, primality testing and factoring. Finally there is a chapter on elliptic curves and their use in cryptosystems and factorization. The book is carefully written, is self-contained, has plenty of exercises (and some nice quotations). With the exception of the final chapter, I would place the level of the book at upper undergraduate rather than postgraduate, and certainly below the level of other texts in Springer's Graduate Texts in Mathematics series (including others by Koblitz). This applies particularly to most of the material in chapter three, some of which would make interesting excercises for a first linear algebra course. This level is perhaps determined more by the mathematical immaturity of the subject, however, rather than by the author's choice of material.

The book concentrates on number theoretic applications to cryptography, and does not try to give a comprehensive introduction to cryptography. Thus one time pads, and block ciphers such as the Data Encryption Standard are not mentioned. As a result, it may be difficult for the reader to appreciate the revolutionary nature of public key cryptosystems. Also, the definitions of one-way and trapdoor functions are confused. No distinction is made between functions whose inverse is always difficult to compute and those having a "trapdoor" where special extra information makes the inverse easy to calculate. Nevertheless, the book contains much material of interest to anyone wanting to broaden the scope of an elementary number theory course, and as such is to be thoroughly recommended.

Finally, mention should be made of the small, ill-spaced typeface used in the book, which can only be described as an assault on the eye. Although it was prepared by the author in camera-

https://doi.org/10.1017/S0013091500028753 Published online by Cambridge University Press